

Texas Cybersecurity Weekly

Collected news & information for Texas' cybersecurity community

Announcements



The Texas Internship Challenge is a partnership between the Texas Workforce Commission (TWC), Texas Education Agency (TEA), and The Higher Education Coordinating Board (THECB), that challenge employers to offer paid internships and make it easy for students to search and apply for them.

Whether you are a student with little to no job experience, or someone looking to change career fields, an internship can provide a path to gaining practical work experience and make full-time employment more attainable in your chosen field. This page contains information on internships for those seeking ways to gain job experience.

[Learn more here →](#)



There continues to be an increased volume of phishing attempts observed over the last several months. State agencies and institutions of higher education should stress users maintain a high level of vigilance when opening attachments or links via email, even if the sender is from within the organization or the email appears to come from a legitimate source. Users should be

cognizant of URLs that do not match hover-text, misleading domain names, poor spelling and grammar, and unexpected requests for action.

A recent incident involved a direction to a malicious Office 365 document. Microsoft describes this malware type and some steps to take. [Read more here](#)

Additionally, phishing growth and maturation can be reviewed in further detail in the [Webroot quarterly](#).

Annual Industry Reports

ENISA Threat Landscape Report 2017



2017 was the year in which incidents in the cyberthreat landscape have led to the definitive recognition of some omnipresent facts. We have gained unwavering evidence regarding monetization methods, attacks to democracies, cyber-war, transformation of malicious infrastructures, and the dynamics within threat agent groups.

ENISA released their annual report in January, available [here](#).

Workforce Development and Events



The TASSCC TEC Conference is a one-day event on April 6 that covers specific topics of interest. Conference attendees will drill down on issues that are relevant and timely to technology directors and specialists alike and

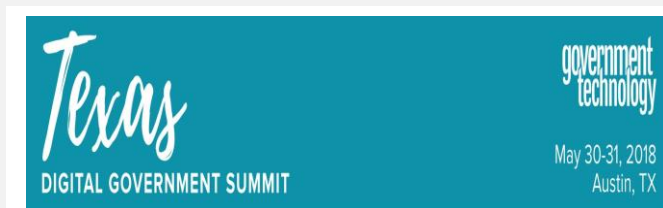
provide an in-depth look at the challenges faced by this community.

[Learn more→](#)



The 18th annual Information Security Forum will be held May 23-24, 2018 at the Palmer Events Center in Austin, Texas, and is hosted by the Texas Department of Information Resources (DIR) and managed by the Office of the Chief Information Security Officer (OCISO).

[Learn more→](#)



Government Technology's passion is helping spread best practices and spurring innovation in the public sector. The Texas Digital Government Summit is designed to do just that. The summit has an advisory board that gathers public and private sector leaders to create an

agenda designed to make that passion relevant and actionable to the state and local government organizations attending the summit.

[Read more→](#)

Threat Alerts



After a cyberattack shut down numerous pipeline communication networks this week, experts are stressing the importance of securing third-party systems in supervisory control and data acquisition (SCADA) environments.

Over the past two days, various major U.S. pipelines across the country reported data system blackouts after a third-party electronic communication system was attacked. That electronic data interchange (EDI) system, which was identified as Energy Services Group's Latitude Technologies Unit, controls computer-to-computer document exchanges with customers.

[Learn more→](#)

Vulnerability Alerts



Multiple Vulnerabilities in Google Android OS Could Allow for Arbitrary Code Execution

MS-ISAC ADVISORY NUMBER: 2018-037

DATE(S) ISSUED: 04/03/2018

Multiple vulnerabilities have been discovered in the Google Android operating system (OS), the most severe of which could allow for arbitrary code execution. Android is an operating system developed by Google for mobile devices, including, but not limited to, smartphones, tablets, and watches. Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution within the context of a privileged process. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

[Learn more→](#)



Multiple Vulnerabilities in PHP Could Allow for Arbitrary Code Execution

MS-ISAC ADVISORY NUMBER: 2018-036

DATE(S) ISSUED: 03/30/2018

Multiple vulnerabilities have been discovered in PHP, the most severe of which could allow an attacker to execute arbitrary code. PHP is a programming language originally designed for use in web-based applications with HTML content. PHP supports a wide variety of platforms and is used by numerous web-based software applications. Successfully exploiting the most severe of these vulnerabilities could allow for arbitrary code execution in the context of the affected application. Depending on the privileges

associated with the application, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploitation could result in a denial-of-service condition.

[Learn more→](#)



Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution

MS-ISAC ADVISORY NUMBER: 2018-035

DATE(S) ISSUED: 03/29/2018

Multiple vulnerabilities have been discovered in iCloud for Windows, Safari, macOS High Sierra, Sierra, and El Capitan, iTunes, Xcode, tvOS, watchOS and iOS. The most severe of these vulnerabilities could allow for arbitrary code execution.

Successful exploitation of the most severe of these vulnerabilities could result in arbitrary code execution within the context of the application, an attacker gaining the same privileges as the logged-on user, or the bypassing of security restrictions. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

[Learn more→](#)

Breach Events



April 1, 2018, NEW YORK & TORONTO--(BUSINESS WIRE)-- HBC (TSX:HBC) today announced that it has become aware of a data security issue involving customer payment card data at certain Saks Fifth Avenue, Saks OFF 5TH, and Lord & Taylor stores in North America. While the investigation is ongoing, there is no indication at this time that this affects the Company's e-commerce or other digital platforms, Hudson's Bay, Home Outfitters, or HBC Europe.

[Learn more→](#)



Panerabread.com, the Web site for the American chain of bakery-cafe fast casual restaurants by the same name, leaked millions of customer records — including names, email and physical addresses, birthdays and the last four digits of the customer's credit card number — for at least eight months before it was yanked offline earlier today...

[Learn more→](#)



Under Armour Notifies MyFitnessPal Users of Data Security Issue

BALTIMORE, March 29, 2018 /PRNewswire/ -- Under Armour, Inc. (NYSE: UA, UAA) today announced that it is notifying users of MyFitnessPal - the company's food and nutrition application and website - about a data security issue. On March 25, the MyFitnessPal team became aware that an unauthorized party acquired data associated with MyFitnessPal user accounts in late February 2018.

[Learn more→](#)

News and Commentaries



Announcing 1.1.1.1: the fastest, privacy-first consumer DNS service

Cloudflare's mission is to help build a better Internet. We're excited today to take another step toward that mission with the launch of [1.1.1.1](#) — the Internet's fastest, privacy-first consumer DNS service.

[Learn more→](#)



The Internet Engineering Task Force (IETF)

The organization that approves proposed Internet standards and protocols— has formally approved TLS 1.3 as the next major version of the Transport Layer Security (TLS) protocol.

This document specifies version 1.3 of the Transport Layer Security (TLS) protocol. TLS allows client/server applications to communicate over the Internet in a way that is designed to prevent eavesdropping, tampering, and message forgery.

[Learn more→](#)

Assistance/Feedback/Questions?

Email the Office of the CISO at
DIRSecurity@dir.texas.gov

The periodical aggregates information about cybersecurity and information technology to promote shared awareness, cyber hygiene, and information sharing amongst government, the private sector, and all Texans.

TLP:WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.